Distillation Protocols that Involve Local Distinguishing: Composing Upper and Lower Bounds on Locally Accessible Information

Aditi Sen(De)[1,2], Ujjwal Sen[1,2], and Maciej Lewenstein[2,3]
[1] *ICFO-Institut de Ciències Fotòniques, E-08860 Castelldefels (Barcelona), Spain*
[2] *Institut für Theoretische Physik, Universität Hannover, D-30167 Hannover, Germany*
[3] *ICREA and ICFO-Institut de Ciències Fotòniques, E-08860 Castelldefels (Barcelona), Spain*

We find a universal lower bound on locally accessible information for arbitrary bipartite quantum ensembles, when one of the parties is two-dimensional. In higher dimensions and in higher number of parties, the lower bound is on accessible information by separable operations. We show that for any given density matrix (of arbitrary number of parties and dimensions), there exists an ensemble, the "Scrooge ensemble", which averages to the given density matrix and whose locally accessible information saturates the lower bound. Moreover, we use this lower bound along with a previously obtained upper bound to obtain bounds on the yield of singlets in distillation protocols that involve local distinguishing.

Distillation of singlets from mixed states is one of the most important protocols in viewing entanglement as a resource in quantum information [1]. It is useful in the key quantum communication tasks like quantum teleportation and quantum dense coding [2]. The discovery of teleportation and dense coding have also initiated the study of quantum channels. In this respect, one of the crucial questions is how much classical information can be encoded in an ensemble of quantum states. In most cases, it is quite hard to find the maximal capacity exactly, and hence the importance of bounds.

There are two main purposes of this paper. *The first purpose* is to find a universal lower bound on the maximal classical information that can be sent to two receivers, when the latter use only local operations and classical communication (LOCC). In a communication protocol in which a source wants to send classical information to a *single* receiver, say Alice, by encoding it in an ensemble of quantum states, important upper and lower bounds have been found on the maximal amount of information that can be extracted by the receiver [3, 4] (see also [5]). In the case when the ensemble is sent to two separated receivers, say Alice and Bob, and whose task is again to gather the maximal information, but now by using only LOCC, an upper bound has also been given [6, 7] (see also [8]). We obtain a universal *lower* bound in the case when at least one of the receivers is constrained to a two-dimensional quantum system. In the case when both parties are with higher dimensional systems, and for the case of higher number of parties, we find the lower bound on the maximal information attainable by separable operations between the receivers. *The second purpose* of the paper is to use the lower bound for obtaining an upper bound on the yield of singlets in any distillation protocol that involves local distinguishing. We will show that indeed such bound can be obtained by using the lower bound of the present paper, and the upper bound of Ref. [7], on maximal classical information obtainable by LOCC (cf. [9]). We indicate that this bound can potentially be used to detect bound entangled states with negative partial transpose [10].

We note here that a two-party system, one of which is two-dimensional is of considerable practical interest, in other domains than considered here. E.g. in the ion trap quantum computer (see e.g. [12]), each ion has two relevant internal states, and is coupled to phonons which are described, strictly speaking by harmonic oscillators, but for any practical purpose, can be described by N-dimensional systems, with large N.

Just as the lower bound in the case of a single receiver [4], required the introduction of the concept of "subentropy", we will have to introduce the concept of "local subentropy". We also show that for any state ϱ (of any dimensions, and any number of parties), the so-called "Scrooge ensemble" [4] corresponding to ϱ, has ϱ as its average ensemble state, and for which the maximal information extractable by LOCC is exactly equal to our lower bound. We also evaluate the bound for some bipartite ensembles, for which the exact value of locally accessible information is not known. It may be worthwhile to note here that upper bounds for the case of a single receiver [3], automatically give upper bounds for the case of multiple receivers. This however is *not* true for the case of a lower bound. In particular, the important lower bound of Ref. [4] for the case of a single receiver, does not give a lower bound for multiple receivers.

Accessible information for a single receiver. Suppose that a source encodes the information about a classical variable x, that occurs with probability p_x, in a quantum state ρ_x, and sends it to a single receiver Alice. Alice therefore receives the ensemble $\mathcal{E} = \{p_x, \rho_x\}$ from the source. Her task now is to gather as much information as possible about x from the ensemble. Let the post-measurement ensemble, after a measurement M that gives outcome y with probability q_y, be $\mathcal{E}^y_{out} = \{p_{x|y}, \rho_{x|y}\}$. The information gathered by Alice from measurement M can be quantified by the mutual information $I_M(\mathcal{E} : M) = H(\{p_x\}) - \sum_y q_y H(\{p_{x|y}\})$, where $H(\{r_i\}) = -\sum_i r_i \log_2 r_i$ is the Shannon entropy of the probability distribution $\{r_i\}$. Thus the mutual infor-

mation is defined by the difference between the initial disorder and the disorder remaining in the final ensemble after performing the measurement, where disorder is quantified by the Shannon entropy. The maximal information, called the accessible information (I_{acc}), that can be gained by Alice is obtained by performing maximization over all measurements: $I_{acc} = \max_M I_M(x:M)$.

Upper and lower bounds for a single receiver. The maximization in accessible information is usually hard to perform, so that it is useful to obtain bounds to estimate it. An upper bound, known as the "Holevo bound" [3], states that $I_{acc} \leq \chi(\mathcal{E}) \equiv S(\rho) - \sum_x p_x S(\rho_x)$, where $\rho = \sum_x p_x \rho_x$ is the average state of the ensemble $\mathcal{E}$, and $S(\sigma) = -\operatorname{tr}\sigma \log_2 \sigma$ is the von Neumann entropy of σ.

Josza, Robb, and Wootters [4] used the notion of subentropy, defined, for a state ρ, as $Q(\rho) = -\sum_k \prod_{l\neq k} \frac{\lambda_k}{\lambda_k - \lambda_l} \lambda_k \log_2 \lambda_k$, with λ_ks being the eigenvalues of the state ρ, to obtain a lower bound: $I_{acc} \geq \Lambda$, where $\Lambda(\mathcal{E}) = Q(\rho) - \sum_i p_i Q(\rho_i)$.

Multiple receivers. Apart from the case of a single receiver, there are other important communication networks. Let us now consider a "$1 \to 2$ quantum network", where a source wants to communicate classical information to two receivers, Alice and Bob. Suppose therefore that the source encodes the classical information x (which occurs with probability p_x in a quantum state ρ_x^{AB} of two particles, e.g. of two photons, and sends the state to Alice and Bob. Alice and Bob, who are at distant locations, obtain the ensemble $\mathcal{E}^{AB} = \{p_x, \rho_x^{AB}\}$. As for the case of a single receiver, their aim is to gather maximal information about x by using local quantum operations and classical communication; in a similar way, one defines the "locally accessible information" (I_{acc}^{LOCC}) by maximizing the mutual information over measurements from this restricted class of operations (LOCC): $I_{acc}^{LOCC} = \max I_M(\mathcal{E}:M)$, where the maximization is performed over all LOCC-based measurement protocols.

Universal upper bound on locally accessible information. Recently, we have shown [7] that for an arbitrary given bipartite ensemble $\mathcal{E}^{AB}$, that produces, after a measurement M, an output (post-measurement) ensemble $\mathcal{E}_{out}$, $I_{acc}^{LOCC} \leq \chi_L(\mathcal{E}^{AB})$, where $\chi_L(\mathcal{E}^{AB}) \equiv S(\rho^A) + S(\rho^B) - \max_{Z=A,B} \sum_x p_x S(\rho_x^Z) - \overline{E}_{out}$, with $\rho_x^{A(B)} = \operatorname{tr}_{B(A)} \rho_x^{AB}$, $\rho^{A(B)} = \sum_x p_x \rho_x^{A(B)}$, and $\overline{E}_{out}$ is an average of an arbitrary asymptotically consistent entanglement measure E for the output states. As discussed before, the Holevo bound also provides an upper bound for I_{acc}^{LOCC}, because $I_{acc}^{LOCC}(\mathcal{E}^{AB}) \leq I_{acc}(\mathcal{E}^{AB}) \leq \chi(\mathcal{E}^{AB})$.

Universal lower bound on locally accessible information. Locally accessible information is defined as a maximization over LOCC-based measurement protocols, and the latter does not have a compact mathematical form. Indeed, the exact value of locally accessible information is known only for a very few ensembles (see e.g. [6, 13], and references therein). Moreover, and in contrast to the case of the upper bound, $\Lambda(\mathcal{E}^{AB})$ is not, in general, a lower bound for I_{acc}^{LOCC}. It is therefore extremely useful to obtain a universal lower bound, to complement the upper bound discussed above.

We obtain the lower bound on locally accessible information by averaging over all measurements on *orthogonal complete pure product bases*. The main obstacle in such an enterprise is that the family of such bases is not well characterised at this moment. On the contrary, it is known that such bases can have quite nonintuitive properties. For example, there exists a complete orthogonal basis of pure product states, which is not distinguishable under LOCC [14]. This will lead to some problems in obtaining the lower bound. However, at least in lower dimensions (precisely in $2 \otimes n$ systems), such problems can be overcome.

Consider therefore a measurement in the complete orthogonal pure product basis $P = \{|\alpha_j\rangle^A \otimes |\beta_k\rangle^B\}$ for a given ensemble $\mathcal{E}^{AB} = \{p_x, \rho_x^{AB}\}$. (We will later on consider the question, whether such a measurement can actually be implemented locally). The mutual information that is gathered in this measurement is given by $I_M(\mathcal{E}^{AB} : P) = H(P) - H(P|\mathcal{E}^{AB})$, where $H(P)$ is the Shannon entropy of the outcome of the measurement in the basis P without a knowledge of the individual states of the ensemble, and $H(P|\mathcal{E}^{AB})$ is the Shannon entropy of the outcome *with* a knowledge of the same. Written out explicitly, $I_M(\mathcal{E}^{AB} : P) = -\sum_{j,k} \langle\alpha_j|\langle\beta_k|\rho^{AB}|\alpha_j\rangle|\beta_k\rangle \log_2 \langle\alpha_j|\langle\beta_k|\rho^{AB}|\alpha_j\rangle|\beta_k\rangle + \sum_x p_x \sum_{j,k} \langle\alpha_j|\langle\beta_k|\rho_x^{AB}|\alpha_j\rangle|\beta_k\rangle \log_2 \langle\alpha_j|\langle\beta_k|\rho_x^{AB}|\alpha_j\rangle|\beta_k\rangle$, where $\rho^{AB} = \sum_x p_x \rho_x^{AB}$ is the average ensemble state.

We now perform the average of $I_M(\mathcal{E}^{AB} : P)$ over all complete orthogonal product measurements. After some simplification, one obtains

$$\begin{aligned}
&\langle I_M(\mathcal{E}^{AB} : P)\rangle = \\
&-d_A d_B \int d\alpha d\beta \langle\alpha|\langle\beta|\rho^{AB}|\alpha\rangle|\beta\rangle \log_2 \langle\alpha|\langle\beta|\rho^{AB}|\alpha\rangle|\beta\rangle \\
&+d_A d_B \sum_x p_x \int d\alpha d\beta \langle\alpha|\langle\beta|\rho_x^{AB}|\alpha\rangle|\beta\rangle \log_2 \langle\alpha|\langle\beta|\rho_x^{AB}|\alpha\rangle|\beta\rangle \\
&\equiv Q_L(\rho^{AB}) - \sum_x p_x Q_L(\rho_x^{AB}) \equiv \Lambda_L(\mathcal{E}^{AB}).
\end{aligned}$$

Here, the ensemble $\mathcal{E}^{AB}$ is from a system of dimensions $d_A \otimes d_B$, and the integrations are over all product states $|\alpha\rangle|\beta\rangle$. Also, $Q_L(\sigma) = -d_A d_B \int d\alpha d\beta \langle\alpha|\langle\beta|\sigma|\alpha\rangle|\beta\rangle \log_2 \langle\alpha|\langle\beta|\sigma|\alpha\rangle|\beta\rangle$, for a bipartite state σ of dimensions $d_A \otimes d_B$. We call $Q_L(\sigma)$ the "local subentropy" of the bipartite state σ. Note that the usual subentropy of Ref. [4] involves an integration over all orthogonal complete measurements, instead of the orthogonal complete *product* measurements in our case. The expression for $Q_L(\sigma)$ can be simplified further to give [4, 15] $Q_L(\sigma) = d_A \int d\alpha Q(\langle\alpha|\sigma|\alpha\rangle) + d_A(\log_2 \mathrm{e})[\frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{d_B}]$, where the argument of Q is supposed to have been normalized to unit trace. Note that in $2 \otimes n$ systems, the remaining integration is just over a single variable.

Using this expression, $\Lambda_L(\mathcal{E}^{AB})$ takes the simple form

$$\Lambda_L = d_A \int d\alpha \left[Q(\langle\alpha|\rho|\alpha\rangle) - \sum_x p_x Q(\langle\alpha|\rho_x|\alpha\rangle) \right]. \quad (1)$$

Since there exists orthogonal complete product bases which cannot be exactly distinguished by LOCC, the corresponding measurements cannot, in general, be implemented by LOCC [14]. However, in dimensions $2 \otimes n$ (for arbitrary n), there exists a simple protocol by which one can implement the measurement onto any orthogonal complete product basis by LOCC [16] (see also [17]). Consequently in $2 \otimes n$, for any ensemble $\mathcal{E}^{AB}$, there exists at least one LOCC-based measurement protocol for which $I_M(\mathcal{E}^{AB} : P) = \Lambda_L(\mathcal{E}^{AB})$, so that in general,

$$I_{acc}^{LOCC} \geq \Lambda_L(\mathcal{E}^{AB}). \quad (2)$$

For the three Bell states $(|00\rangle \pm |11\rangle)/\sqrt{2}$, $(|01\rangle + |10\rangle)/\sqrt{2}$ (with equal probabilities), the upper bound in Ref. [6], and the lower bound here, give $0.2515 \leq I_{acc}^{LOCC} \leq 1$.

In higher dimensions (e.g. in $3 \otimes 3$), $\Lambda_L(\mathcal{E}^{AB})$ is a lower bound of accessible information under a larger family of operations, called the family of "separable superoperators". A separable superoperator is one which transforms bipartite states σ^{AB}, defined on the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$, as $\sigma \to \sum_i A_i \otimes B_i \sigma A_i^\dagger \otimes B_i^\dagger$, where A_i and B_i are operators on $\mathcal{H}_A$ and $\mathcal{H}_B$ respectively, such that $\sum_i A_i^\dagger \otimes B_i^\dagger A_i \otimes B_i$ equals the identity operator on $\mathcal{H}_A \otimes \mathcal{H}_B$. Note that implementation of the measurement onto any complete orthogonal product basis is a separable superoperator. In the case of higher number of parties, the generalization of the definition of Q_L, that considers measurements on complete orthogonal product bases of all the parties, provides also a lower bound on accessible information with separable superoperators.

Bound on entanglement distilable via protocols that involve distinguishing. We now consider distillation protocols that involve a (local) distinguishing process, which *may or may not* correct all errors. Suppose therefore that Alice and Bob share m copies of the state $\varrho^{AB} = \sum_i p_i (|\psi_i\rangle\langle\psi_i|)^{AB}$, where the $|\psi_i\rangle$ may or may not be mutually orthogonal. Consider now the following distillation protocol. Alice and Bob share some string of the form $|\psi_{i_1}\rangle \otimes \ldots \otimes |\psi_{i_m}\rangle$ with probability $p_{i_1} \ldots p_{i_m}$; the corresponding ensemble being called $\mathcal{E}_{\varrho,m}$. They try to obtain the information on the string they share. This is for example the case in the hashing protocol [11]. For such protocols, we have $\Lambda_L(\mathcal{E}_{\varrho,m}^{\to 2}) \leq I_{acc}^{LOCC}(\mathcal{E}_{\varrho,m}^{\to 2}) \leq I_{acc}^{LOCC}(\mathcal{E}_{\varrho,m}) \leq \chi_L(\mathcal{E}_{\varrho,m})$, where $\mathcal{E}_{\varrho,m}^{\to 2}$ is the ensemble $\mathcal{E}_{\varrho,m}$, projected on a suitably chosen $2 \otimes n$ subspace. Considering now the entanglement measure E in χ_L to be the distillable entanglement, we obtain

$$D \leq S(\varrho^A) + S(\varrho^B) - \overline{S}_A - \Lambda_L(\mathcal{E}_{\varrho,m}^{\to 2})/m,$$

where D is the average entanglement distilled, per copy, in the protocol considered above, and $\overline{S}_A = \sum_i p_i S(\mathrm{tr}_{B \text{ or } A} |\psi_i\rangle\langle\psi_i|)$. Note that the bound is valid both in the asymptotic regime, as well as in the nonasymptotic one, with the latter being more important in most practical applications. For Bell-diagonal states (i.e. states ϱ that are diagonal in the canonical maximally entangled basis [18]) in $d \otimes d$, we have

$$D \leq \log_2 d - \Lambda_L(\mathcal{E}_{\varrho,m}^{\to 2})/m,$$

and the result is compatible with the hashing yields [11].

In Ref. [7], we proposed a different bound on entanglement distillable in certain protocols; the one here, however, has a larger range of applicability, as the former was only for distillation protocols that fully distinguish the strings, which e.g. requires mutually orthogonal $|\psi_i\rangle$'s. Even in the case of the hashing protocol, which uses orthogonal $|\psi_i\rangle$'s (the Bell states), the distinguishing is typically not complete [11].

Note that the method of obtaining the upper bound on D, can be used for other future lower bounds on I_{acc}^{LOCC}. In particular, a lower bound that can be of the order $\log_2 d$, can potentially be used to detect bound entangled states with negative partial transpose [10].

Special cases. It is sometimes possible to further simplify the expression for Λ_L given in Eq. (1). E.g., consider the case when the average ensemble state ρ^{AB} is a product state, i.e. it is of the form $\rho^A \otimes \rho^B$. This can happen for example in the cases when we want to evaluate the lower bound for a complete orthogonal ensemble of (not necessarily product) states. We can then simplify the first term of $\Lambda_L(\mathcal{E}^{AB})$ (see Eq. (1)) as follows:

$$\begin{aligned} & \Lambda_L(\mathcal{E}^{AB}) \\ = \; & -d_A d_B \{ Q(\rho^A) + Q(\rho^B) - (\log_2 \mathrm{e})[(\frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{d_A}) \\ - \; & (\frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{d_B})] \} + \text{2nd term}. \end{aligned} \quad (3)$$

This simplification will help us to calculate the lower bound for any complete ensemble of orthogonal states.

This happens e.g. in the case of the ensemble $\mathcal{E}_1$ in $2 \otimes 2$, consisting of the four orthogonal states (given with equal probabilities) $|\psi_1\rangle = a|00\rangle + b|11\rangle + c|10\rangle$, $|\psi_2\rangle = k[(b-c)|00\rangle + (c-a)|11\rangle + (a-b)]|10\rangle$, $|\psi_3\rangle = x|00\rangle + y|11\rangle + z|10\rangle$, $|\psi_4\rangle = |01\rangle$, where a, b, c are real numbers, $k = 1/\sqrt{(b-c)^2 + (c-a)^2 + (a-b)^2}$, and x, y, z are suitable real values, satisfying the normalization condition $x^2 + y^2 + z^2 = 1$, and orthogonality conditions of $|\psi_3\rangle$ with $|\psi_1\rangle$ and $|\psi_2\rangle$. The exact locally accessible information for this ensemble is not known. Again, the average state for this ensemble is the identity in the four dimensional complex Hilbert space, and hence is of the form $\rho^A \otimes \rho^B$. In Fig. 1, we draw the lower bound on locally accessible information with respect to a single parameter (using Eq. (3)).

If we have an ensemble consisting of only pure product states (not neccessarily orthogonal), and for which the

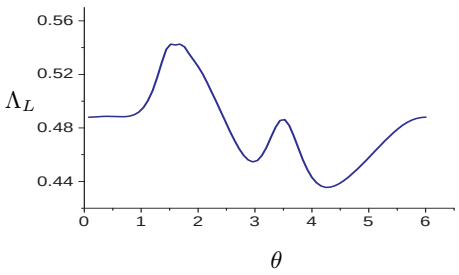

FIG. 1: The lower bound for the ensemble $\mathcal{E}_1$. We set $a = \sin\theta/2\cos\phi/2$, $b = \sin\theta/2\sin\phi/2$, $c = \cos\theta/2$, with $\phi = \pi/4$.

average ensemble state is of the form $\rho^A \otimes \rho^B$, the lower bound can be further simplified as $\Lambda_L = Q(\rho^A) + Q(\rho^B)$. An example of this situation is an ensemble consisting of $|00\rangle, |01\rangle, |10\rangle, |11\rangle, |{+}{+}\rangle, |{+}{-}\rangle, |{-}{+}\rangle, |{-}{-}\rangle$ (with equal probabilities), where $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$.

Saturation. We now show that for any given multiparty density matrix ρ (of any dimensions), there exists an ensemble (called the Scrooge ensemble [4]), for which the average state is ρ, and $I_{acc}^{LOCC} = \Lambda_L$. Let $\{|e_i\rangle\}_{i=1}^N$ ($\{\lambda_i\}_{i=1}^N$) be the eigenbasis (eigenvalues) of ρ. The eigenbasis may contain entangled states. Then the Scrooge ensemble $\mathcal{E}_\mathcal{S}$ is the (continuous) distribution of $|\{x_i\}\rangle = \sum_i \sqrt{x_i}|e_i\rangle$, distributed as $(n-1)!ndx_1 \ldots dx_{N-1}/[\lambda_1 \ldots \lambda_{N-1}(x_1/\lambda_1 + \ldots + x_N/\lambda_N)^{N+1}]$. It was shown in Ref. [4] that the amount of mutual information that is obtained in a complete orthogonal measurement on $\mathcal{E}_\mathcal{S}$ is a constant. Therefore, the mutual information obtained by measuring onto any *multi-orthogonal* complete product basis will be a constant ($= Q_L(\mathcal{E}_\mathcal{S})$), and such measurement can be performed locally for any dimensions and any number of parties. Finally, the maximal mutual information for *global* measurements is, in general, attainable on complete measurements [19], so that for $\mathcal{E}_\mathcal{S}$, $I_{acc}^{LOCC} = Q_L$ (because I_{acc}^{LOCC} is sandwiched between I_{acc} and Q_L, in this case). To our knowledge, this is the only known globally indistinguishable ensemble for which $I_{acc} = I_{acc}^{LOCC}$.

Summary. We have obtained a universal lower bound on locally accessible information for arbitrary bipartite ensembles, in the case when one of the parties has a two-dimensional system. For higher dimensional and multipartite systems, the universal bound is for separable operations. We have shown that for any given multiparty state ρ there exists an ensemble whose local accessible information saturates our bound, and whose average state is ρ. We use this lower bound along with a previously obtained upper bound on the same quantity, to give an upper bound on the yield of singlets in distillation protocols that involve local distinguishing.

We acknowledge support from the DFG (SFB 407, SPP 1078, SPP 1116, 436POL), the Alexander von Humboldt Foundation, the EC Program QUPRODIS, the ESF Program QUDEDIS, and EU IP SCALA.

[1] M.A. Nielsen and I.L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).
[2] C.H. Bennett *et al.*, Phys. Rev. Lett. **70**, 1895 (1993); C.H. Bennett and S.J. Wiesner, *ibid.* **69**, 2881 (1992).
[3] J.P. Gordon, in *Proc. Int. School Phys. "Enrico Fermi, Course XXXI"*, ed. P.A. Miles, pp 156 (Academic Press, NY 1964); L.B. Levitin, in *Proc. VI National Conf. Inf. Theory, Tashkent*, pp 111 (1969); A.S. Holevo, Probl. Pereda. Inf. **9**, 3 1973 [Probl. Inf. Transm. **9**, 110 (1973)]; H.P. Yuen, in *Quantum Communication, Computing, and Measurement*, ed. O. Hirota *et al.* (Plenum, NY 1997)); B. Schumacher, M. Westmoreland, and W. K. Wootters, Phys. Rev. Lett. **76**, 3452 (1996).
[4] R. Josza, D. Robb, and W. Wotters, Phys. Rev. A, **49**, 668 (1994).
[5] S.R. Nichols and W.K. Wootters, quant-ph/0207010; F. Mintert and K. Życzkowski, Phys. Rev. A **69**, 022317 (2004).
[6] P. Badziąg, M. Horodecki, A. Sen(De), and U. Sen, Phys. Rev. Lett. **91**, 117901 (2003).
[7] M. Horodecki, J. Oppenheim, A. Sen(De), and U. Sen, Phys. Rev. Lett. **93**, 170503 (2004).
[8] S. Ghosh, P. Joag, G. Kar, S. Kunkri, and A. Roy, Phys. Rev. A **71**, 012321 (2005).
[9] J. Eisert *et al.*, Phys. Rev. Lett. **84**, 1611 (2000).
[10] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. 80, 5239 (1998); P. Horodecki, Phys. Lett. A 232, 333 (1997); D.P. DiVincenzo *et al.*, Phys. Rev. A 61, 062312 (2000); W. Dür, J. I. Cirac, M. Lewenstein, and D. Bruß, *ibid.* 61, 062313 (2000).
[11] C.H. Bennett *et al.*, Phys. Rev. Lett. **76**, 722 (1996); C.H. Bennett, D.P. DiVincenzo, J.A. Smolin, and W.K. Wootters, Phys. Rev. A **54**, 3824 (1996); K.G.H. Vollbrecht and M.M. Wolf, *ibid.* **67**, 012303 (2003).
[12] J.I. Cirac and P. Zoller, Phys. Rev. Lett. **74**, 4091 (1995); J.F. Poyatos, J.I. Cirac, and P. Zoller, *ibid.* **81**, 1322 (1998).
[13] J. Walgate, A.J. Short, L. Hardy, and V. Vedral, Phys. Rev. Lett. **85**, 4972 (2000); S. Virmani, M.F. Sacchi, M.B. Plenio, and D. Markham, Phys. Lett. A **288**, 62 (2001); Y.-X. Chen and D. Yang, Phys. Rev. A **64**, 064303 (2001); **65**, 022320 (2002); J. Walgate and L. Hardy, Phys. Rev. Lett. **89**, 147901 (2002); D. Bruß, G.M. D'Ariano, M. Lewenstein, C. Macchiavello, A. Sen(De), and U. Sen, Phys. Rev. Lett. **93**, 210501 (2004).
[14] C. H. Bennett *et. al.*, Phys. Rev. A **59**, 1070 (1999).
[15] S. Sykora, J. Stat. Phys. **11**, 17 (1974); K.R.W. Jones, J. Phys. A **24**, 1237 (1991).
[16] C.H. Bennett *et al.*, Phys. Rev. Lett. **82**, 5385 (1999); D.P. DiVincenzo *et al.*, Comm. Math. Phys. **238**, 379 (2003).
[17] S. Virmani and M. B. Plenio, Phys. Rev. A **67**, 062308 (2003).
[18] The canonical maximally entangled basis in $d \otimes d$ are $\frac{1}{\sqrt{2}}\sum_{i=0}^{d-1} e^{2\pi ijn/d}|j\rangle|(j+m)\text{mod } d\rangle$, $(n, m = 0, \ldots, d-1)$.
[19] E.B. Davies, IEEE Trans. Inform. Th. **IT24**, 596 (1978).